

## EXECUTIVE SUMMARY

On 25 and 26 August 2004, the United States Army War College's Center for Strategic Leadership, in partnership with George Washington University, conducted the symposium, "In Support of the Common Defense: Examining Critical Infrastructure Protection in the Public and Private Sector." The symposium was divided into four panels, each followed by a moderated question and answer session. The panels focused upon the direction and intent of the Federal government in its strategies and policies toward critical infrastructure and key resources (CI/KR) protection; the impact of those strategies and policies on the Department of Defense (DoD), State and local governments, and the private sector; the demands of building effective partnerships for infrastructure protection between the public and private sectors; and means of measuring the effectiveness of our protective programs. In addition to these panels, a keynote address was delivered by the Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense, who focused on the challenge of moving critical infrastructure protection beyond the defense culture of the Cold War.

### **Panel 1: Critical Infrastructure Protection Strategies: The Direction and the Intent**

#### **"Formulating Strategies for Critical Infrastructure Protection"**

The symposium began with Professor Bert Tussing of the U.S. Army War College offering a presentation on formulating strategies for Critical Infrastructure Protection (CIP). He pointed out the importance of tying CIP strategies to the series of "senior" security strategies in order to ensure continuity of purpose and provide a foundation for the prioritization of efforts. For the United States, this begins with the National Security Strategy (NSS)—the "grand strategy," designed to pursue the national objectives delineated to secure our interests and preserve our values.

## IN SUPPORT OF THE COMMON DEFENSE

The NSS is “supported” by a series of implementing strategies, to include the National Military Strategy (NMS), the Department of State Strategic Plan, and—of particular importance to the discussion—the National Strategy for Homeland Security (NSHS). In turn, the NSHS has its own set of implementing strategies for infrastructure protection: the National Strategy to Secure Cyberspace and the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. The “ends, ways, and means” of these strategies necessarily draw upon those presented in the senior documents they support. Indeed, a strategic concept presented in the NSHS may reappear as a strategic objective in the National Strategy to Secure Cyberspace. This association provides an automatic review process in developing the subordinate strategies, and an inherent means of prioritizing efforts and resources for the larger task of national security. “There is a continuity of direction and purpose that should be displayed in our strategies that will be essential not only in terms of efficiencies, but equally in terms of effectiveness.”

### “Senior Leader Assessment”

Dr. Kent Butts continued the forum by presenting observations gleaned from a Senior Symposium held on Critical Infrastructure Protection, conducted at the Army War College in May of 2004. The symposium was attended by seven retired general officers and senior civilian officials, from both the public and the private sectors, all actively involved in homeland security issues.

The panel conceded that identification and prioritization of critical infrastructure were the first great challenges to be overcome before the country could begin an earnest effort to protect it, but that significant obstacles lay in the way of those preliminary tasks. The first obstacle lies in framing the requirements as a national issue, rather than a Federal requirement. The “management mission” of critical infrastructure protection should go to the State and local government. These will bear a significant share of the job of identifying and prioritizing assets, and a substantial piece of protecting them, with the Federal government in support. The Federal government, in turn, must provide a degree of specificity in what constitutes criticality in the prioritization efforts.

The senior panel examined the relations between the government and the private sector in CIP. They noted that currently the most effective

## IN SUPPORT OF THE COMMON DEFENSE

means of liaison between these elements may be the Information Sharing and Analysis Centers (ISACs) associated with eleven critical infrastructure sectors. The problem is that the ISACs, wholly voluntary in nature, vary markedly in their constituent participation and their effectiveness. The Federal government could enhance the strength and cooperative benefit of their ISAC partners (and the private sector as a whole) by clearing the procedural obstructions to information sharing, and offering incentives to accompany regulations and standards for “hardening” our infrastructure against terrorist attacks.

The senior forum paid a great deal of attention to the evolving role of the National Guard in homeland defense/homeland security. The participants were unanimous in their stance that the proximity of the Guard and their relationships with the American community make them the logical “first line of defense” in the battle for homeland security, and that homeland defense should well be the “primary” mission of the Guard. They noted, however, that commitment levels being borne by the Guard—in Iraq or elsewhere—could eventually impact this primary responsibility of providing “rear area security for the states.” In particular, the participants warned that the impact being felt among civilian first responders, which populate much of the National Guard’s rolls, could eventually lead to a backlash from the states, leading to calls for limits on the “overseas commitment” of the force.

### **“Homeland Security Presidential Directive 7 (HSPD-7): The Drafter’s Intent”**

The forum’s first panel concluded with a presentation by Mr. Michael Gilmore of the Government Accountability Office, addressing the lineage and intent of government policies and strategies addressing critical infrastructure and key resource protection. Mr. Gilmore began with a reassertion of the fact that protection must be viewed as a national commitment, rather than Federal responsibility, shared by Federal, State, and local governments, as well as the private sector. In order to facilitate that partnership, the Federal government has identified thirteen infrastructure sectors, each led by a Sector-Specific Agency (SSA), charged with coordinating both the governmental and public-private cooperation that will be essential in ensuring asset and systems protection.

## IN SUPPORT OF THE COMMON DEFENSE

Mr. Gilmore noted that, until recently, the government's attention was mainly devoted to protecting infrastructure and resources against natural disasters. The current environment has forced us to realign existing programs and systems to address manmade threats to those entities, stretching across a spectrum ranging from negligence to deliberate malevolence. He made particular mention of the relatively unheralded "insider threat," which—against all intuition—has grown to be the most frequently identified threat to these realms.

In keeping with the direction of the first panel, Mr. Gilmore conducted a brief review of the most significant "policy documents" associated with the Federal government's component of the national effort toward infrastructure protection. The review began with an acknowledgement of Presidential Decision Directive 63 (PDD-63) from the Clinton Administration, and continued through the recommendations of the Presidential Commission on Critical Infrastructure Protection (Oct 97), the Homeland Security Act of 2002, the NSHS (Jul 02), the National Strategy to Secure Cyberspace (Feb 03), and the National Strategy for the Physical Protection of Critical Infrastructure and Key Resources (Feb 03). Each of these contributed to the direction of HSPD-7 (Dec 03) which both supercedes the provisions of PDD-63 and provides for the implementation of the strategies which preceded it. This directive clarifies the actions required by the Homeland Security Act, defines responsibilities for the Department of Homeland Security (DHS) and other sector specific agencies, and provides guidance for the interaction between those agencies, State and local governments, and the private sector. It is the Federal government's foundational directive for identifying, prioritizing and protecting critical infrastructure in the United States.

### **Keynote Address: The Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense**

Mr. McHale began with an assertion that our concerns for critical infrastructure protection must be reflective of the fundamental changes in the nature of the threat against that infrastructure. In the past, our concerns were always directed toward a destructive power that was only available to nation-states. Now we face a new era of terror that has made the same potential for destruction available to non-state entities, even

## IN SUPPORT OF THE COMMON DEFENSE

individuals, which has exponentially complicated our efforts to prevent, prepare for, and respond to this type of devastation.

The Secretary delivered an overview of the changes that have occurred in the Federal government to address this new threat, highlighting particularly the establishment of the Department of Homeland Security, the U.S. Northern Command (NORTHCOM), and his own assistant secretariat within the DoD. He noted, also, some of the changes that may be in store for the Intelligence Community in their efforts to focus more on the domestic threat in our War on Terrorism, especially following the recommendations of the 9/11 Commission.

Just as the Intelligence Community is reconfiguring for a new global environment, our direction toward infrastructure protection must be reviewed and reengineered, Mr. McHale declared. He suggested that we are currently “stuck” in a Cold War mentality surrounding our defense of vital resources and assets, focusing on traditional civil engineering concepts of redundancy, systems analysis, single points of failure and the like. These remain vital, but must be reinforced by unique approaches to an asymmetric threat. He noted especially an urgent requirement to frustrate the ability of our enemies to reconnoiter and collect data with an eye toward identifying and exploiting vulnerabilities to domestic targets.

Mr. McHale outlined a number of questions, yet to be answered, that will significantly impact the face of infrastructure protection, especially from the perspective of the DoD. The role of NORTHCOM in CIP has yet to be defined, as well as the manner in which that role will mesh with the command’s Antiterrorism/Force Protection mission. The operational role of the National Guard in this area is also in formulation; and how the Guard will work in consonance with NORTHCOM, the active component, and the remaining elements of the Nation’s reserve component will require carefully planning and scrutiny. The Secretary alluded to recent innovations in the command and control of the Guard in concert with Title 10 forces—innovations played out to great success at last summer’s G-8 summit and both the Democratic and Republican National Conventions—that could have important implications to the CIP mission. Finally, Mr. McHale contended that we need to better define Defense Critical Infrastructure. In spite of existing definitions, the lines have become blurred as we attempt to distinguish between that

## IN SUPPORT OF THE COMMON DEFENSE

infrastructure which is owned by DoD and that infrastructure upon which DoD depends.

### **Panel 2: Critical Infrastructure Protection Strategies: The Effect**

#### **“The View from the Pentagon”**

The second panel began with a presentation by Mr. William Bryan, Director for Critical Infrastructure in the Office of the Assistant Secretary of Defense for Homeland Defense. Mr. Bryan began by reminding the audience that “criticality” in critical infrastructure protection is time and situation dependent. What may not appear to be vulnerable at one time and place in an existing set of circumstances could quickly become so under different circumstances. Likewise, an infrastructure which could be a prime candidate for attack under one set of conditions could be viewed by the enemy as unassailable under another. This distinction was made to reinforce the importance of not only identifying critical resources in need of protection, but prioritizing that need in a fluctuating environment, and then realizing that those priorities might change.

Mr. Bryan listed the major initiatives being taken by DoD for CIP, including the Integrated Risk Management Strategies for CIP and the Defense Industrial Base (DIB), and the sector-specific plan for DIB being developed by DoD in support of the National Infrastructure Protection Plan mandated by HSPD-7. In spite of these initiatives, he warned that our focus may be drawing too much toward process and not enough toward protection. More differentiation is required between our traditional “all-hazards” approach to CIP, in order to address a more focused and insidious threat. Terrorism, he reminded the audience, “is a hazard that thinks.”

Mr. Bryan also reminded the participants that DoD is faced with a unique set of “global CIP concerns,” which complicate an already difficult intelligence/information challenge at home and abroad. In that light, he paid homage to the importance of building upon the relationship the Department has always enjoyed with the Intelligence Community, and to nurture that relationship in new venues. He particularly mentioned the importance developing a more effective relationship with those elements

## IN SUPPORT OF THE COMMON DEFENSE

of Information Assurance and Infrastructure Protection Directorate of DHS that deal with intelligence analysis and dissemination, and reiterated the importance of our strengthening information sharing mechanisms throughout the CIP community.

The Director suggested that one means of lowering the risk to critical infrastructure and key resources may lie in remembering that protection is not our only option. Remediation, mitigation, redundancy and other preemptive measures designed around our critical infrastructure and key resources are still available to us. These are measures that have served us in the past, and while they may not address all that is entailed in the new threat to our infrastructure, they should not be overlooked.

### **“Executing the National Vision from State and Local Government”**

Mr. Donald Keldsen of the Maryland Emergency Management Agency offered a candid assessment of the Federal government’s CIP initiatives from a state’s perspective. He characterized initiatives sent down to State and local governments as frequently resulting in confusion, frustration, huge expenditures of manpower, and little in the way of tangible results. The direction has all too often been ambiguous and uncoordinated as, to date, the Federal government has been unable to clarify what and how much of the infrastructure needs to be protected, and from what.

Mr. Keldsen, a retired Army Colonel, pointed to what he saw to be another aspect of misunderstanding with regard to the role of the National Guard: to wit, a prevailing assumption in State and local governments that the Guard is ready and configured to perform a “critical asset protection program.” The truth is that the Full Spectrum Integrated Vulnerability Assessment (FSIVA) program the states are hanging their collective hats upon is focused on the DoD’s mission as sector-specific agency charged with the protection of the DIB—not the other twelve key infrastructure sectors, nor the four key resource areas. This is leaving too many government officials with the falsest sense of security, in the belief that a set of responsibilities not even addressed by the Guard is a job “already done.”

Mr. Keldsen charged that vulnerability assessments in general have been duplicative, costly in terms of time, manpower and resources, and devoid of substantial benefit toward critical infrastructure protection.

## IN SUPPORT OF THE COMMON DEFENSE

Citing three successive iterations of assessments launched by DHS' Office of Domestic Preparedness (ODP), he charged that focus changed from a "train-the-trainer" approach to a Federal-trainer tactic. In the first instance, he opined that a lack of guidance left no clear idea of what constituted "critical infrastructure" from one locality to another. In the latter, he charged that the focus evolved to recovery and response, but little in the way of preventative infrastructure protection. As a result of the first two assessments, Maryland "passed" on an invitation by ODP to revalidate earlier assessments.

With regard to public-private sector interaction, Mr. Keldsen charged that efforts toward cooperation at the State and local level could only be described as "superficial." The reason for this weakness is that there has been no real mandate for this cooperation and that the preponderance of cooperative effort that has occurred to date has been achieved simply as a matter of goodwill. He conceded that there is a lot of Federal interaction going on with the private sector, but State and local jurisdictions have trouble establishing CIP plans with infrastructure concerns that "do not necessarily stop at the State border." This condition is exacerbated by the fact that the State is finding itself outside of the "information and coordination loop" between the public (read "Federal") and private sector.

In sum, Mr. Keldsen found the Federal intent fighting against obstacles constructed by its own "fragmented approach." A comprehensive, integrated plan substituting clear direction, concrete methodologies and predictable resourcing for "conceptual" guidance is needed. Without these, he contends, "we can't get there."

### **"Partnering in Defense Industrial Base Protection"**

The final presentation on the panel was made by Mr. William V. Ennis, Director of the Industrial Analysis Center of the Defense Contract Management Agency (DCMA). Mr. Ennis's presentation spoke to the unique requirements of a private sector that is most intimately involved in national defense: the Defense Industrial Base. A reflection of its importance is the fact that the DoD is charged as the SSA for overseeing the identification, prioritization, and protection of assets within its infrastructure. Mr. Ennis noted the efforts underway in the evolving partnership between DoD and the DIB. Information sharing is a most compelling issue for the private sector, encompassing concerns

## IN SUPPORT OF THE COMMON DEFENSE

over the protection of proprietary and other unclassified, albeit sensitive, information. DoD will require department policy, and in some cases statutory authority, to govern the protection of this information.

Mr. Ennis also commented on initiatives to share the burden of remediation between the department and its industrial base. Working with asset owners, the Department will develop alternative courses of action to mitigate or remediate vulnerabilities once they are identified. The course of action to be taken from among these will be selected based on the nature and immediacy of a threat, affordability, and other practical concerns.

The preponderance of Mr. Ennis' presentation was devoted to describing operational initiatives that DCMA has undertaken to meet protection requirements for the DIB. He noted that DoD is focusing on reducing the magnitude of assets contained in the DIB to a manageable number for prioritization and protection through a process that begins by examining all prime contractors and subcontractors and systematically chooses selected sites and facilities based on varying measures that define their criticality. He noted that "the list," once established, remains dynamic, with DoD reviewing, updating, and approving site prioritization on a semiannual basis.

Once DoD identifies a critical DIB asset, it must conduct vulnerability assessments to determine risks and to determine if those critical assets are, indeed, vulnerable. If DoD and its DIB partner identify significant vulnerabilities, they will collaborate to develop alternative courses of action to mitigate or remediate the threat, and will share in the decision to implement a remedy.

Currently DoD is developing a set of standards to conduct FSIVAs which will apply to DIB assets. The effort builds on current vulnerability assessment efforts, and will employ means for self-assessments as they reveal themselves. These self-assessments, when they are developed, will support, but not act as a substitute for scheduled FSIVAs conducted by the Department. Mr. Ennis presented a series of factors that will determine when, how, and by whom the scheduled assessments will occur.

Mr. Ennis introduced the Integrated Industrial Capability Risk Assessment Process to the forum, posing it as a complementary effort to other assessment and prioritization initiatives. The process is divided into

## IN SUPPORT OF THE COMMON DEFENSE

Industrial Capability Assessments, Technology Assessments, and Financial Assessments. These assessments analyze capabilities, technologies and financial data to identify problem areas and develop resolution alternatives in order to fulfill future national security requirements. Mr. Ennis's presentation ended with a case study showing how remediation efforts developed following a financial and technological assessment could provide the Department with an alternative to physical security protection.

### **Panel 3: The Public-Private Partnership in Critical Infrastructure Protection**

#### **“Challenges of the Partnership: Pulling together the Public and the Private Sectors”**

The first presentation of the third panel was made by Ms. Marilyn Ware, Chairman of Ware Family Offices and Chairman Emeritus of American Water. Ms. Ware began by saying that, since 9/11, the country has been engaged in a homeland security continuum that started with an evaluation process of our vulnerabilities, continued to an adaptation process that has seen the establishment of DHS and initiatives such as HSPD-7 and the National Infrastructure Protection Plan (NIPP), and has subsequently advanced to a transition stage. The transition stage, by far the most difficult, will not be successful until the public and private sectors can address their differences in risk aversion, in performance-based rewards, and in divergent approaches to competition.

Ms. Ware suggested that CI/KR protection would have to be a function of public-private sector partnerships on a Federal, State, and local basis. This national problem would logically begin with the DHS organizing the effort, but would have to engage other governmental entities, academia and the private sector to coordinate the process from organization to implementation. In that regard, she holds that the Federal government has primary responsibility for governance in the necessary private-public infrastructure protection partnerships; that State government has primary cognizance over accountability; and that local government, with their private sector partners, will hold principal responsibility for implementation of security measures designed to protect CI/KR. She noted, however, that every level of government participation

## IN SUPPORT OF THE COMMON DEFENSE

in these partnerships, up to and including regulation, must be carefully planned in partnership with infrastructure sector participants to avoid excessive disruption and add value to the sector.

Ms. Ware pointed to several extant mechanisms that will facilitate the public-private partnership and the security environment. The National Infrastructure Advisory Council (NIAC), established by order of the President, is charged specifically with enhancing the partnerships in terms of protecting the information systems that underpin all CI/KR protection issues. The eleven private-sector ISACs serve as principal mechanisms to share strategic, operational and tactical information among sector entities and between the sectors and DHS. The Sector Coordinating Councils, mandated by HSPD-7, may characterize the future of sector coordination and information sharing activities, and DHS's Homeland Security Information Network (HSIN) may become a "self-contained, one-stop shop" for assimilation and dissemination of threat and risk assessments. An important aspect of all of these is that they represent mechanisms for local input into Federal policy, as well as points of entry for government into sector-level infrastructure protection activities and issues.

As the Nation transitions to what Ms. Ware refers to as "partnership readiness," she opines that the private sector will engage in risk management planning and invest in security as a necessary business function. In implementing the NIPP, it will be called upon to follow sector-specific infrastructure protection plans, and work with Federal, State, and local governments to identify and implement best practices, develop performance metrics and information sharing mechanisms, and ensure cross sector coordination. At the same time, government must remain keenly aware of their private sector partners' ultimate responsibility to shareholders who expect a return on investment and consumers who expect products and services. These obligations, too, are fundamental, "since without consumer demand, reasonable profits, strong cash flow, and a healthy balance sheet, there simply will be no private sector with whom to partner."

### **"Sticks and Carrots: Incentives and Regulations for the Private Sector"**

Mr. Al Martinez-Fonts, Special Assistant to the Secretary for the Private Sector, Department of Homeland Security, was the next presenter

## IN SUPPORT OF THE COMMON DEFENSE

on the panel. Mr. Martinez-Fonts began by describing the unique mandate of his office, calling for a staff of fifteen personnel to promote information sharing and best practices and to build partnerships within the twenty-five million businesses currently existing in the United States. Within DHS he is the principal advocate of the private sector and ensures that the Secretary remains keenly aware of the implications of public policy decisions on that sector.

Mr. Martinez-Fonts described the primary goal of his office as proving the business case for homeland security. Businesses must be led to conclude that expenditures toward additional security in a new era of terror must be viewed as an investment, not an expense.

Having said that, Mr. Martinez-Fonts echoed the position espoused throughout the conference: that the public-private partnership that will be essential for real CI/KR protection must be characterized by a balance between commerce and security, and that the balance must prove profitable. He pointed to a number of initiatives being taken by the government that are a clear indication of the need for this profitable balance, including Customs Trade Partnership Against Terrorism (CTPAT), Free and Secure Trade (FAST), and the Maritime Transportation Safety Act. At the same time, he suggested that some measures taken in the name of enhanced security should be reexamined in terms of unintended consequences. He noted particularly an assessment made by the Private Sector Senior Advisory Committee to the Secretary of Homeland Security that identified new obstacles in visa processing as the number one “security related” cost to business in the country today.

In spite of this progress, Mr. Martinez-Fonts remains convinced that, in many ways, the government neither understands the requirements of the private sector, nor the private sector those of the government. In order to close that gap of understanding, the government must present private industry with a value proposition. Some things by necessity will have to be mandated/regulated, but most “best practices” should be left to voluntary implementation. Information sharing should be facilitated beyond procedural obstacles (such as overly stringent clearance requirements) in a responsible manner, but one which still conveys the notion that the government is indeed interested in sharing situational

## IN SUPPORT OF THE COMMON DEFENSE

awareness of issues of interest—and potential danger—to their private sector partners.

Finally, Mr. Martinez-Fonts suggested that if the government were really interested in proving the importance of their partnership in CIP and other endeavors, they should find some means of providing relief to the specter of liability suits against the private sector. In the current environment, it is wholly possible that some measure of advancing domestic security from the private sector is being neglected due to fear of litigation turned against a business engaged in “doing the right thing.” In this environment of sometimes frivolous litigation reasonable risks are not being taken, new products are not being developed and new concepts are going unheard.

### **“Breaching the Trust Barrier: Information Sharing for the Common Defense”**

The final presenter on the “Public-Private Partnership” panel was Mr. Harrison D. Oellrich, Managing Director of Guy Carpenter and Company, Inc. Mr. Oellrich addressed the unique role that the insurance sector (and more specifically, the reinsurance community) had assumed in the country’s concern for CIP. Given the nature of a growing domestic threat, reinsurance provides conventional insurers with the capacity, stability, financing and/or protection from catastrophe.

Mr. Oellrich noted that a difficulty the community is currently facing, however, is in developing probabilistic and deterministic modeling for terrorist attacks that will provide insurers and reinsurers a necessary basis for their protection. This type of modeling exists for addressing natural catastrophes; but the industry is plagued by a lack of risk management needed for providing predictability to inherently unpredictable acts of deliberate terrorism.

Mr. Oellrich reiterated a frequently voiced position at the conference over reticence from within the private sector over information sharing with the Federal government, even after an attack has occurred. Proprietary information, and more importantly, customer confidence, has often deterred businesses that have experienced attacks against their infrastructure (especially surrounding information systems) from reporting those attacks. Until the government can persuade these

## IN SUPPORT OF THE COMMON DEFENSE

businesses that data surrounding attacks of this nature would be protected, this reticence is likely to remain.

In the course of his presentation, Mr. Oellrich suggested that there were three ways the government can influence the private sector to maintain and enhance measures contributing to national security: by way of regulation, by way of persuasion through coaxing or cajoling, and by way of incentives. If incentives can be devised, he suggested, the government stands a better chance of enlisting all of the strengths of the private sector. Mr. Oellrich suggested that the insurance and reinsurance industries, themselves, could assist in providing incentives toward this end.

Mr. Oellrich acknowledged that the government was making concerted efforts to bring about working partnerships with the private sector for CIP, but he outlined three challenges that would have to be overcome if those partnerships were to have a chance to succeed. First, government must find a means of counteracting the “transient” nature of its representatives in order to instill the necessary confidence required for this public-private partnership. Secondly, cultural awareness will have to be established between the public and private sectors, to effectively communicate and pursue common interests in what is sometimes seen as parallel but distinct universes. And finally, open communications characterized by enhanced information sharing initiatives from both sides will have to be realized as a foundational prerequisite for breaching the “trust gap” between government and private industry.

### **Panel 4: The Challenge Under Examination**

#### **“Critical infrastructure Protection: Mapping Threats Against Vulnerabilities”**

The first presenter in the final panel of the conference was Mr. Jon MacLaren, of the Protective Services Division of DHS’ Information Assurance and Infrastructure Protection (IAIP) Directorate. Mr. MacLaren based his discussion on the five-step Risk Management Methodology by which the Department intends to construct its critical infrastructure/key resource protection plan across the private and public sectors.

## IN SUPPORT OF THE COMMON DEFENSE

- Identifying Critical Infrastructure through the utilization of the evolving national database
- Assessing Vulnerabilities
  - Against specific intelligence about potential/imminent threats
  - Against postulate threats in the absence of specific intelligence
- Normalizing, Analyzing, and Prioritizing through analytical techniques to generate “relative risk profiles” by which protection initiatives may be prioritized
- Implementing protective programs through collaboration with key partners in the public and private sectors
- Measuring Effectiveness through Performance Metrics focusing particularly on the speed and efficiency of information sharing, and the level of interaction between the public and private sectors during program implementation

Mr. MacLaren pointed out that, while these five steps will enable the Federal government to lead the way in addressing challenges to CI/KR, the execution of the various protection initiatives would always occur locally. Moreover, he reminded the assemblage that the private sector must assume much of its own lead in risk management for proper buy-in to occur and for the CIP programs to succeed. In that light, Mr. MacLaren challenged the members of the audience from the private sector to lift risk management and enterprise security concerns to board level cognizance. “Good security must be seen as good business,” he concluded, but that vision would only be sustainable through the private sector “from the top down.”

### **“Measured Response: Computational Experimentation and Training Environment for Homeland Security”**

Next, Dr. Alok Chaturvedi, Director of Purdue University’s Homeland Security Institute, offered an example of how elements of the academic community were simulating attacks and devising protective solutions through modeling and simulation. Specifically, the doctor briefed the symposium on Measured Response, a simulation training exercise series conducted at Purdue to facilitate the decision-making challenges facing

## IN SUPPORT OF THE COMMON DEFENSE

Federal, State, and local government officials in coordinating response strategies against terrorist strikes in the U.S.

The central mechanism in the Measured Response exercise series was the Synthetic Environment for Analysis and Simulations (SEAS) platform. Developed by Dr. Chaturvedi and Shailendra Mehta of the Kannert School of Management, SEAS allows the creation of fully functioning synthetic economies, societies, nations, and organizations that mirror the “real world.” The program includes means of replicating geography and physical details like road networks, traffic patterns, structures, and the like, and incorporates role sets that guide the interaction of agents in the model. From that interaction, SEAS provides for a depiction of the consequences of a given action, thus providing a laboratory for testing the efficiency of policies, strategies, and other decision tools of the public-private partnership for infrastructure protection.

A particularly interesting application of SEAS was demonstrated in its use as a conceptual model for computation experimentation in bio-terrorism. Dr. Chaturvedi explained that the model mimicked essential demographic, epidemiological, and economic characteristics of the U.S., and developed detailed simulations of city, state, and national command centers. Using that environment, the exercise was able to simulate a biological attack on a synthetic population, subsequently portraying human response against consequences on a local, state, and national level.

The purpose of the exercise was to allow decision makers to practice resource and risk management under crisis. Specifically, Dr. Chaturvedi noted six key objectives:

- To practice resource/risk management under an unconventional crisis situation
- To examine prioritization, timing, and intensity tradeoffs of response decisions and actions
- To exercise emergent communication strategy development and enhancement
- To practice real-time incident management and allocation of decision making among different levels of government

## IN SUPPORT OF THE COMMON DEFENSE

- To develop/exercise execution and effort coordination among different agencies and actors
- To practice management of public mood and expectations

### **“The Defense Critical Infrastructure Protection Program: A Mission Assurance Solution”**

The last formal presentation of the symposium was delivered by Mr. Dan Mathis, Deputy Program Manager and Director of Operations of the Defense Program Office for Mission Assurance. The presentation offered a brief overview of DoD’s Defense Critical Infrastructure Protection (DCIP) program, responsive to the requirements for DoD delineated in HSPD-7.

Mr. Mathis described DCIP as a comprehensive set of goal-driven activities that identify and prioritize assets deemed essential to the execution of the NMS, assess vulnerabilities to the same, and manage associated risks that are revealed in those assessments. The DCIP is a complementary program linking the mission assurance aspects of DoD’s Anti-Terrorism/Force Protection (AT/FP), Information Assurance (IA), Continuity of Operations Plan (COOP), and other readiness programs.

The DCIP is concerned with three classes of infrastructure and their associated assets:

- DoD-owned infrastructure and assets that support the NMS
- Non-DoD infrastructures and assets that support the NMS, such as the DIB and commercial infrastructure that provides power, communications, transportation and other utilities that DoD must rely upon to meet operational needs
- Non-DoD infrastructure and assets so vital to the Nation that their incapacitation, exploitation or destruction could have a debilitating effect on the security or economic well-being of the Nation, or could negatively affect national prestige, morale, and confidence

In providing for the protection of these three classes, DoD has developed the DCIP Integrated Risk Management Strategy for FY 2006-2011. The Strategy consists of five major elements, each with specified goals and initiatives.

## IN SUPPORT OF THE COMMON DEFENSE

1. Understand Risks
  - Goal: Identify Critical Assets and Dependencies and the impact of the degradation or loss
  - Goal: Conduct Vulnerability and Risk Assessments
2. Implement the Protection Program
  - Goal: Act on Remediation and/or Mitigation recommendations
3. Respond to Incidents
  - Goal: Effectively support Incident Management
4. Provide Adequate Program Support
  - Goal: Ensure an effective Critical Infrastructure Program foundation
5. Enable Management Initiatives
  - Goal: Institutionalize DoD CIP policy and the DCIP program
  - Goal: Provide and Manage adequate program resources
  - Goal: Foster Department-wide collaboration

Mr. Mathis stated that the elements, goals and initiatives outlined in the DCIP are all directed toward an objective of significantly reducing the vulnerabilities of assets critical to DoD missions using a structured systems engineering, and risk-based management process. A key component of that process is DCIP's vulnerability assessment mechanism, the FSIVA. Modular in nature, the FSIVA program allows assessment teams to conduct appraisals of system vulnerability in eleven different types of systems, ranging from Physical Security to Supporting Infrastructure Networks. Once vulnerabilities are identified and analyzed against known threats, the impact of the loss of a specific asset is determined and potential mitigation or remediation strategies for the system are developed. Vulnerabilities, threats, and potential solutions are then added to the DCIP Management System, which is made available to combatant commanders, services, agencies, and associated stakeholders in the infrastructure sectors.

Mr. Mathis concluded his presentation by introducing symposium participants to DCIP's risk assessment formula,  $R=I*(V*T)$ , wherein:

## IN SUPPORT OF THE COMMON DEFENSE

R=risk, I = Impact, V= vulnerabilities, and T= threat/hazard

He reported that the application of threat information against known asset vulnerabilities, and the impact of loss or diminished capacity of those assets, provides a current view of risk to the same and, ultimately, to mission accomplishment. As threats against a particular asset come and go and as the severity of potential impact rises and falls, so too will risk rise and fall. The understanding of this risk permits remediation decisions and, when necessary, provides for the prioritized selection of critical assets to protect.

IN SUPPORT OF THE COMMON DEFENSE

